REMARKS/ARGUMENTS

The present amendment is responsive to the Office Action dated June 29, 2006. Claims 6-9, 16-19, 26-29 and 36-39 have been amended to refer to non-cancelled claims. No new matter has been introduced by these amendments. Claims 2-5, 12-15, 22-25 and 32-35 were previously canceled. The Examiner has withdrawn claims 45 and 46 in the Office Action. Therefore, claims 1, 6-11, 16-21, 26-31, and 36-44 are again presented for consideration in view of the following remarks. A petition for a one-month extension of time is submitted herewith.

Reexamination and reconsideration of the above-identified application, pursuant to and consistent with 37 C.F.R. § 1.116, and in light of the remarks that follow, are respectfully requested. Because the present claims are believed to be in condition for allowance over the cited art, good cause exists for the entry of this reply in accordance with 37 C.F.R. § 1.116.

As indicated above, the Examiner has withdrawn claims 45-46, which were introduced in the prior amendment dated March 16, 2006. Applicants respectfully traverse the restriction.

According to the Office Action, independent claims 1, 11, 21 and 31 "merely recite 'unique terminal identification information being selected in a manner unrelated to the authentication data', which is more broad than 'assigning the MAC address', recited in the newly added claims 45 & 46. Also, the additionally recited, 'validating, transferring, retrieving and transferring steps', are directed to a specific software installation algorithm, which is beyond the scope of the claims as previously presented." (Office Action, pg. 2, numbered section 1.)

There are two criteria for a proper restriction requirement. First, the two inventions must be independent or

distinct. And second, a "serious burden" would be placed on the Examiner if restriction were not required. M.P.E.P. § 803. Neither of these criteria has been met.

As to the first criteria, the Office Action makes no mention of the fact that claims 45 and 46 require "recognition data" that is unique to the client device, as well as a unique address (the MAC address) which is unrelated to the recognition data. These limitations are generally related to those presented in claims 1, 11, 21, and 31, although they may be of different scope. However, claims of differing scope are not necessarily independent or distinct.

As to the second criteria, the Office Action makes no mention of any search burden placed on the Examiner. However, "the examiner, in order to establish reasons for insisting upon restriction, must explain why there would be a serious burden on the examiner if restriction is not required." M.P.E.P. § 808.02.

Applicants submit that there is no search burden. As indicated above, claims 45 and 46 may be of different scope from the other claims in the case, but they include closely related features. And features such as the "MAC address" of these claims are in dependent claims that have already been examined. Specifically, claims 41-44 depend from independent claims 1, 11, 21 and 31, respectively, and all refer to the unique terminal information comprising a MAC address.

Thus, applicants submit that there is no proper reason for withdrawing claims 45 and 46 from the instant application, and respectfully request that these claims be considered on the merits.

Claims 6-9, 16-19, 26-29 and 36-39 were rejected under 35 U.S.C. § 112, ¶ 2 for depending upon a cancelled claim. As stated above, these claims have been amended to properly depend

from respective independent claims 1, 11, 21 and 31. Therefore, applicants respectfully request that the rejection be withdrawn.

Claims 1, 6-11, 16-21, 26-31, and 36-44 were rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 5,862,220 ("*Perlman*") in view of U.S. Patent No. 6,049,671 ("*Slivka*"). Applicants respectfully traverse the rejection.

Claim 1 recites, among other limitations, "receiving ***authentication data associated with said one receiving terminal***; authenticating said authentication data; transmitting ***unique terminal information identifying said one receiving terminal as a destination*** of transmission and an update program to change the processing of said one receiving terminal, ***said unique terminal identification information being selected in a manner unrelated to said authentication data***, and said transmitting step including ***converting said unique terminal information into converted unique terminal information comprising a key ID*** and transmitting said converted unique terminal information to said one receiving terminal."

Claim 11 recites, among other limitations, "a transmission apparatus operable to receive ***authentication data associated with one of said plurality of receiving terminals***, to authenticate said authentication data, and to ***transmit unique terminal information identifying said one receiving terminal as a destination*** of transmission and an update program to change the processing of said one receiving terminal; said one receiving terminal being operable to output said authentication data, to receive said unique terminal information and said update program, to communicate with said transmission apparatus via an Internet system, and to receive a digital broadcasting signal, and said one receiving terminal including a specified storage location operable to store said unique terminal

information and said update program to update said processing; ***wherein said unique terminal identification information is selected in a manner unrelated to said authentication data***, and said transmission apparatus transmits ***said unique terminal information converted into a key ID*** to said one receiving terminal and said one receiving terminal converts said converted unique terminal information back to said unique terminal information and then stores said unique terminal information in said storage location."

Claim 21 recites, among other limitations, "a plurality of receiving terminals, one of said plurality of receiving terminals being operable to ... output ***authentication data associated with said one receiving terminal***, and, upon authentication of said authentication data by said transmission apparatus, to ***receive unique terminal information identifying said one receiving terminal as a destination*** of transmission and an update program for changing the processing of said one receiving terminal; ... a transfer request generated based on said update program and transmitted to the transmission apparatus along with said unique terminal information; and data responsive to said transfer request supplied by the transmission apparatus to said one receiving terminal based on said unique terminal information; ***wherein said unique terminal information is selected in a manner unrelated to said authentication data***, and ***converted unique terminal information is obtained by converting said unique terminal information into a key ID***."

And claim 31 recites, among other limitations, "receiving ***unique terminal information identifying said one receiving terminal as a destination*** of transmission and an update program for changing the processing of said one receiving terminal, ***said unique terminal identification information being***

selected in a manner unrelated to authentication data associated with said one receiving terminal; converting said unique terminal information into a key ID; storing said unique terminal information and said update program received by said one receiving terminal in a storage location; transmitting said unique terminal information and a transfer request based on said update program from said one receiving terminal to said transmission apparatus; and receiving data transmitted from said transmission apparatus in response to said transfer request based on said unique terminal information."

The Office Action asserts that *Perlman* discloses the majority of the features of the pending claims. For instance, with regard to independent claims 1, 11, 21 and 31, the Office Action states that "receiving authentication data associated with the one receiving terminal, authenticating the authentication data', reads on the disclosure in *Perlman*, which uses a WebTV telephone number with an ANI, in order to determine if the client is listed on the server, for authentication purposes." (Office Action, pg. 4, numbered section 6.)

Perlman does disclose use of ANI, or Automatic Number Identification, "for security verification and authentication purposes." (Col. 4, ll.51-52.)

> ANI can be a effective tool for verifying the location from which a network access is being made. For example, a WebTV client network interface device 610 may access the WebTV network server 620 to request a particular type of service. In some circumstances, it is necessary or desirable to verify a client's identity before performing the requested service. Telephone network services such as Caller ID and **Automatic Number Identification (ANI) can be used to provide a requesting client's telephone number to the WebTV server 620.** This can be performed transparently to the client user. The WebTV **server 620 may use the requesting client's telephone number to authorize the completion of a requested service** by comparing the

> requesting client's telephone number to a list of authorized telephone numbers maintained in the server 620. If the requesting client's telephone number is on the server list, the requested service is completed for the client. If the requesting client's telephone number is not on the server list for the requested service, the client is notified that the requested service cannot be performed. Since ANI and Caller ID cannot be faked by a surreptitious user, this feature of the present invention allows the WebTV network to provide a significant level of security for network transactions. This authentication feature is described in more detail in the following sections.
>
> (Col.4, l.53 to col.5, l.10, emphasis added.)

Clearly, the ANI feature discussed in *Perlman* is integrally related to the client's telephone number. The Office Action goes on to state that the "claimed 'unique terminal identification information', reads on the client network address stored on the private server 820 and provided back to the client 610, col. 8, lines 35-44." (*Id.*) The Office Action subsequently states that the "'unique terminal identification information being selected in a manner unrelated to the authentication data..." also reads on the disclosure in *Perlman* that in at least one embodiment the client device 610 is authenticated using its POTS number, col. 8, lines 30-67." (*Id.* at pg. 5.)

In these relied-upon portions of *Perlman*, the reference states:

> Referring now to FIG. 11, a flow chart illustrates the processing performed by a WebTV client 610. The logic illustrated in FIG. 11 is used by a client 610 to establish a secure data communication link with a WebTV server 620 over a conventional unsecure data network. In a first processing step 1110, client 610 performs a power-up initialization. Next, client 610 connects to private server 820 over a secure network line 858. Once client 610 is connected with private server 820, client 610 requests the private server 820 to determine the client network

address of client 610. Because it is not always possible for client 610 to determine its own network address, this information must be requested from private server 820. If access by client 610 to conventional network 612 is performed using a standard POTS telephone network, **private server 820 can use conventional automatic number identification (ANI) functionality to obtain the telephone number from which client 610 is calling. In the POTS telephone network situation, this client telephone number represents the client network address from which the client 610 is accessing the network.** Once the private server 820 obtains the client network address, this client network address is stored on private server 820 and/or provided back to the requesting client 610. In addition, the private server 820 generates an encryption key for the client 610. This encryption key is specific to that particular client and is used for encrypting subsequent data communications between client 610 and WebTV server 620 (processing block 1112).

Referring now to FIG. 12, the private server 820 processing logic is illustrated. In processing block 1210, the private server 820 receives a request from a client 610 for a determination of the client's network address and the generation of an encryption key for the client. **The private server 820 uses conventional techniques to obtain the client network address in processing block 1212**. In the case of a POTS telephone network connection between private server 820 and client 610, **private server 820 uses conventional automatic number identification (ANI) techniques to obtain the client telephone number from where the telephone call to the private server 820 originated.** In the preferred embodiment, private server 820 provides a known (800) telephone number which a client 610 may use to access private server 820. Once this connection to private server 820 is made, the network address determination logic 910 of private server 820 uses standard telephone ANI functionality to determine the telephone number or network address of the client 610 which originated the telephone call (processing block 1212).

(Col.8, ll.21-67.)

Thus, in the recited examples, Perlman utilizes ANI to

obtain the client's telephone number. It bears repeating that "In the POTS telephone network situation, this client telephone number represents the client network address," as quoted above. Therefore, while the Office Action cites to two separate portions of *Perlman* as disclosing the claimed authentication data and unique terminal identification information, it should be clear that this is not the case. In the independent claims, the unique terminal identification information is selected in a manner unrelated to authentication data. However, *Perlman* discloses the opposite - namely using the client's telephone number for both ANI-based authentication and for the client network address.

The Office Action also asserts that "[a]s for the 'key ID', *Perlman* furthermore teaches that the encryption key is specific to the particular client, col. 8, lines 39-47." (Office Action, numbered section 6, pg. 5.) This section of *Perlman* states:

> Once the private server 820 obtains the client network address, this client network address is stored on private server 820 and/or provided back to the requesting client 610. ***In addition, the private server 820 generates an encryption key for the client 610. This encryption key is specific to that particular client*** and is used for encrypting subsequent data communications between client 610 and WebTV server 620 (processing block 1112).
>
> (Col.8, ll.39-47, emphasis added.)

However, this is not what is claimed. Rather, independent claims 1, 11, 21 and 31 require "converting said unique terminal information into converted unique terminal information comprising a key ID", "said unique terminal information converted into a key ID," "converted unique terminal information is obtained by converting said unique terminal

information into a key ID," and "converting said unique terminal information into a key ID," respectively. The cited portion of *Perlman* does not disclose converting anything similar to unique terminal information into a key ID.

Slivka has been extensively discussed in responses to prior Office Actions, which are incorporated by reference herein. In view of the prior responses, applicants submit that *Slivka* does not overcome any of the aforementioned deficiencies of *Perlman*.

Accordingly, it is respectfully submitted that claims 1, 11, 21, and 31 patentably distinguish over *Perlman* and *Slivka*, both individually and in the combination that the Office Action suggests can be made therefrom. Accordingly, applicants respectfully request reconsideration and allowance of independent claims 1, 11, 21, and 31.

Furthermore, claims 6-10, 16-20, 26-30 and 36-44 depend from claims 1, 11, 21, and 31, respectively, and contain all the limitations thereof. Accordingly, applicants submit that the subject dependent claims are likewise patentable.

In view of the above, each of the presently pending claims in this application is believed to be in immediate condition for allowance. Accordingly, the Examiner is respectfully requested to withdraw the outstanding rejection of the claims and to pass this application to issue.

If, however, for any reason the Examiner does not believe that such action can be taken at this time, it is respectfully requested that he telephone applicants' attorney at (908) 654-5000 in order to overcome any additional objections which he might have. If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 12-1095 therefor.

Dated: October 16, 2006

Respectfully submitted,

By _____

Andrew T. Zidel
Registration No.: 45,256
LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK, LLP
600 South Avenue West
Westfield, New Jersey 07090
(908) 654-5000
Attorney for Applicant

700402_1.DOC